

CLAIMS

What is claimed is:

1. A method of creating a digitally stored digital certificate, the method comprising the steps:

5 defining in said certificate a protected area;
storing at least one digital component in said protected area;
calculating a digital value as a function of digital content stored in said protected area;

and

10 storing a digital signature in said certificate but outside said protected area, said digital signature being encrypted and a function of said value.

2. A method according to claim 1 wherein said protected area is defined by storage of framing characters.

15 3. A method according to claim 2 wherein said certificate includes line elements, and at least one of said line elements begins with one of said framing characters and ends with one of said framing characters.

20 4. A method according to claim 1 wherein said at least one component comprises a tag field and at least one of a length field and a data field.

5. A method according to claim 4 wherein said data field includes only characters from a restricted character set.

25 6. A method according to claim 5 wherein said restricted character set corresponds to a subset of an ASCII code character set.

30 7. A method according to claim 4 wherein said data field is a binary-based data converted from a binary data set to a restricted character set.

8. A method according to claim 7 wherein said restricted character set is a subset of an ASCII code character set.

35 9. A method according to claim 7 wherein said converted binary-based data is converted to said restricted character set by encoding according to base-64 encoding.

10. A method according to claim 1 wherein said value is a message digest value.

40 11. A method according to claim 1 wherein said value is calculated by application of a hashing algorithm to characters only in said protected area.

12. A method according to claim 1 wherein said digital signature is converted from a binary data set to a restricted character set.

13. A method according to claim 12 wherein said restricted character set is a subset of an ASCII code set.

14. A method according to claim 12 wherein said converted digital signature is converted to said restricted character set by encoding according to base-64 encoding.

5
SUB A2
15. A digitally stored digital certificate comprising:
a digital storage medium;
a digital certificate data structure stored upon said storage medium, said data structure
10 defining a protected area;
at least one digital component stored in said protected area;
a digital signature stored in said certificate data structure but outside said protected area,
said digital signature being encrypted and a function of said at least one digital component stored
in said protected area.

15
16. A digital certificate according to claim 15 wherein said protected area is established by storing framing characters in said digital certificate data structure.

20
17. A digital certificate according to claim 16 wherein said certificate data structure includes line elements, and at least one of said line elements begins with one of said framing characters and ends with one of said framing characters.

25
18. A digital certificate according to claim 15 wherein said at least one component comprises a tag field and at least one of a length field and a data field.

19. A digital certificate according to claim 18 wherein said data field includes only characters taken from a restricted character set.

30
20. A digital certificate according to claim 19 wherein said restricted character set corresponds to a subset of an ASCII code character set.

21. A digital certificate according to claim 21 wherein said data field is a binary-based data converted from a binary data set to a restricted character set.

35
22. A digital certificate according to claim 21 wherein said restricted character set is a subset of an ASCII code character set.

23. A digital certificate according to claim 21 wherein said converted binary-based data is converted to said restricted character set by encoding according to base-64 encoding.

40
24. A digital certificate according to claim 15 wherein said value is a message digest value.

45
25. A digital certificate according to claim 15 wherein said value is calculated by application of a hashing algorithm to characters only in said protected area.

26 A digital certificate according to claim 15 wherein said digital signature is converted from a binary data set to a restricted character set.

27 A digital certificate according to claim 26 wherein said restricted character set is a subset of an ASCII code set.

28. A digital certificate according to claim 26 wherein said converted digital signature is converted to said restricted character set by encoding according to base-64 encoding.

29. A digitally stored digital certificate of product ownership of a given product by a given product owner, said certificate comprising:

a digital storage medium;

a digital certificate data structure stored upon said storage medium, said data structure defining a protected area;

a first digital component stored in said protected area and identifying said given product;

a second digital component stored in said protected area and identifying said given product owner;

a digital signature in said certificate data structure but outside said protected area, said digital signature being encrypted and a function of at least said first and second components stored in said protected area.

30. A digital certificate according to claim 29 wherein said protected area is established by storing framing characters in said digital certificate data structure.

31. A digital certificate according to claim 30 wherein said certificate data structure includes line elements, and at least one of said line elements begins with one of said framing characters and ends with one of said framing characters.

32. A digital certificate according to claim 29 wherein said value is a message digest value.

33. A digital certificate according to claim 29 wherein said value is calculated by application of a hashing algorithm to content of said protected area.

34. A digital certificate according to claim 29 wherein said digital signature is converted from a binary data set to a restricted character set.

35. A digital certificate according to claim 34 wherein said restricted character set is a subset of an ASCII code set.

36. A digital certificate according to claim 34 wherein said converted digital signature is converted to said restricted character set by encoding according to base-64 encoding.